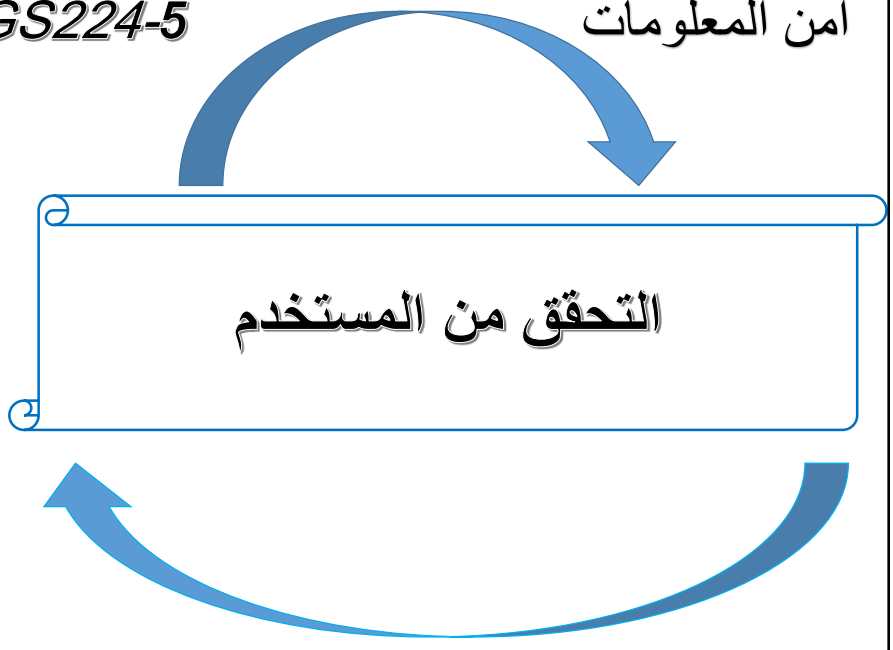
أمن المعلومات GS224-5



التحقق من المستخدم

يعتبر التحقق من المستخدم هو اللبنة الأساسية للأمن وخط الدفاع الأول. (أساس التحكم في الوصول ومحاسبة المستخدم)

"عملية التحقق من الهوية المدعى بها كيان نظام أو لصالحه"

- تتكون عملية المصادقة من خطوتين:
  - **التعريف**: تقديم المعرف لنظام الأمان. (يجب تعيين المعرف بعناية ، لأن الهويات المصادق عليها هي أساس خدمات الأمان الأخرى ، مثل خدمة التحكم في الوصول)
  - **التحقق:** تقديم أو إنشاء معلومات المصادقة التي تؤكد الارتباط بين الكيان والمعرف.
- في جوهرها ، المعرف هو الوسيلة التي يقدم المستخدم من خلالها هويته المزعومة للنظام ؛ مصادقة المستخدم هي وسيلة إثبات صحة الادعاء. لاحظ أن مصادقة المستخدم تختلف عن مصادقة الرسائل (عندما تهتم الأطراف المتصلة بسلامة تبادل الرسائل).

وسائل التحقق من المستخدم

أربع وسائل لمصادقة هوية المستخدم ، والتي يمكن استخدامها بمفردها أو مجتمعة: أساسها هو شيء الشخص :

- **يعرفه** ، على سبيل المثال كلمة المرور ، رقم التعريف الشخصي (PIN).
- **يمتلكه** ، على سبيل المثال البطاقات الذكية والمفتاح المادي .
- **يجسده** (القياسات الحيوية الثابتة) ، على سبيل المثال التعرف على بصمات الأصابع وشبكية العين والوجه.
- **يقوم به** (القياسات الحيوية الديناميكية) ، على سبيل المثال التعرف عن طريق الصوت والتوقيع وإيقاع الكتابة.
- يمكن استخدامها بمفردها أو مجتمعة لتحقيق هوية المستخدم.
- كل طريقة لديها مشاكل. قد يتمكن الخصم من تخمين كلمة المرور أو سرقتها. قد يكون الخصم قادرًا على تزوير أو سرقة البطاقة. قد ينسى المستخدم كلمة مرور أو يفقد رمزًا مميزًا. علاوة على ذلك ، هناك عبء إداري كبير لإدارة كلمات المرور ومعلومات البطاقات على الأنظمة وتأمينها في الأنظمة. مع المصادقات البيومترية (القياسات الحيوية) ، هناك مجموعة متنوعة من المشاكل ، بما في ذلك التعامل مع الإيجابيات الزائفة والسلبيات الكاذبة، وتقبل المستخدم لها ، والتكلفة ، والراحة.

تقييم اخطار التحقق من المستخدم

- **مستوى التأكيد**: درجة اليقين من أن المستخدم قد قدم بيانات اعتماد تشير إلى هويته المدعية:
  - المستوى-1: ثقة قليلة (منتدى عبر الإنترنت)
  - المستوى-2: بعض الثقة (المنظمات المهنية)
  - المستوى-3: ثقة عالية (المتقدمون بمكتب براءات الاختراع)
  - المستوى-4: ثقة عالية جدًا (الموظفون يتعاملون مع خدمات خطيرة/حساسة)
- **التأثير المحتمل**: منخفض ، متوسط ، كبير .

التحقق من المستخدم بواسطة كلمة المرور

- طريقة لتحقق من المستخدم منتشرة على نطاق واسع
  - يقدم المستخدم الاسم/تسجيل الدخول وكلمة المرور
  - يقارن النظام كلمة المرور بتلك المحفوظة لتسجيل الدخول المحدد
- مصادقة معرف تسجيل المستخدم و أن المستخدم مصرح له بالدخول إلى النظام ويحدد صلاحيات المستخدم، ومقدار التحكم بالوصول.
- نظام كلمة المرور يعتبر خط الدفاع الأمامي ضد المتسللين. جميع الأنظمة المتعددة المستخدمين تطلب من المستخدم ألا يقدم اسمًا أو معرفًا فحسب ، بل كلمة مرور أيضًا. يقارن النظام كلمة المرور بكلمة المرور المخزنة مسبقًا لمعرف هذا المستخدم ، والمحفوظة في ملف كلمات المرور في النظام. تعمل كلمة المرور على مصادقة معرف تسجيل الدخول الفردي إلى النظام. بدوره ، يحدد المعرف ما إذا كان المستخدم مصرحًا له بالوصول إلى نظام ، والصلاحيات الممنوحة للمستخدم ، ويستخدم لتحديد ضوابط الوصول التقديرية.

نقاط ضعف كلمة المرور

- **هجوم القاموس:** قد يتجاوز المتسلل ما عناصر التحكم في الوصول ويحصل على حق الوصول إلى ملف كلمات المرور في النظام ، ثم يقارن المهاجم تجزئة كلمة المرور مقابل تجزئات كلمات المرور الشائعة الاستخدام.
- **هجوم على الحساب محدد:** يستهدف المهاجم حسابًا معينًا ويرسل تخمينات كلمة المرور حتى يتم اكتشاف كلمة المرور الصحيحة .
- **هجوم كلمة المرور الشائع**: يختار المهاجم كلمة مرور شائعة ويجربها ضد مجموعة واسعة من معرفات المستخدم.
- **تخمين كلمة المرور لمستخدم واحد:** يحاول المهاجم اكتساب معلومة حول صاحب الحساب وسياسات كلمة مرور النظام ويستخدم هذه المعلومة لتخمين كلمة المرور.
- **اختطاف محطة العمل** ؛ ينتظر المهاجم محطة عمل نشطة الى حين تركها مفتوحة التسجيل (نشطة بدون وجود مستخدم).
- **استغلال أخطاء المستخدم**: إذا قام النظام بتعيين كلمة مرور ، فمن المرجح أن يقوم المستخدم بتدوينها لأنه من الصعب تذكرها.
- **استغلال استخدام كلمة مرور متعددة**: عندما تشترك أجهزة شبكة مختلفة في نفس كلمة المرور أو كلمة مرور متماثلة لمستخدم معين.
- **المراقبة الإلكترونية:** إذا تم إرسال كلمة مرور عبر شبكة لتسجيل الدخول إلى نظام بعيد ، فإنها تكون عرضة للتنصت.

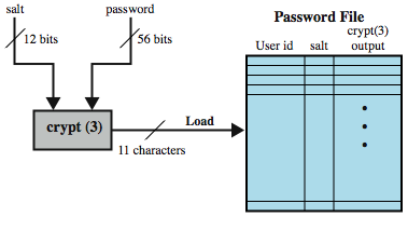
الإجراءات المضادة لاختراقات كلمة المرور

تشمل الإجراءات المضادة للثغرات الأمنية ضوابط من أجل:

- منع الوصول غير المصرح به إلى ملف كلمة المرور ،
- تدابير كشف التسلل لتحديد الاختراق ، وإعادة إصدار كلمات المرور بسرعة في حالة اختراق ملف كلمة المرور ،
- آلية قفل الحساب التي تمنع الوصول إلى الحساب بعد عدد من محاولات تسجيل الدخول الفاشلة ،
- سياسات ضد استخدام كلمات المرور الشائعة ولكن استخدام كلمات المرور يصعب تخمينها ،
- التدريب و فرض سياسات كلمات المرور التي تجعل من الصعب تخمين كلمة المرور،
- تسجيل خروج من محطة العمل تلقائيًا بعد فترة من عدم النشاط ،
- سياسة تحظر نفس كلمة المرور أو كلمة مرور مشابهة على أجهزة شبكة معينة ؛ تشفير الاتصالات.
- من المفيد دراسة / البحث عن نقاط ضعف كلمات المرور لان طريقة كلمات المرور تعتبر الاكثر انتشارا ولا تزال الأكثر كفاءة .

استخدام كلمات المرور المجزأة (Hashed passwords)

تقنية أمان لكلمة المرور المستخدمة على نطاق واسع هي استخدام كلمات المرور المجزأة (hashed passwords) والقيمة المضافة (salt value)، ومستخدمة في نظام التشغيل يونيكس وعلى عدد من أنظمة التشغيل الأخرى، والطريقة موضحة في الشكل (أ). لتحميل كلمة مرور جديدة في النظام ، يقوم المستخدم بتحديد كلمة مرور أو تعيينها. يتم دمج كلمة المرور هذه مع قيمة مضافة ذات طول ثابت (بحيث يمكن لكلمة مرور المستخدم نفسها إنشاء قيم تجزئة متعددة ، اعتمادًا على القيمة المضافة للمستخدم ، لجعل الهجمات أكثر صعوبة). في التطبيقات القديمة ، ترتبط القيمة المضافة بالوقت الذي يتم فيه تعيين كلمة المرور للمستخدم. تستخدم التطبيقات الأحدث عددًا عشوائيًا . تعمل كلمة المرور والقيمة المضافة كمدخلات لخوارزمية التجزئة لإنتاج رمز تجزئة ثابت الطول. تم تصميم خوارزمية التجزئة لتكون بطيئة في التنفيذ لإحباط الهجمات.

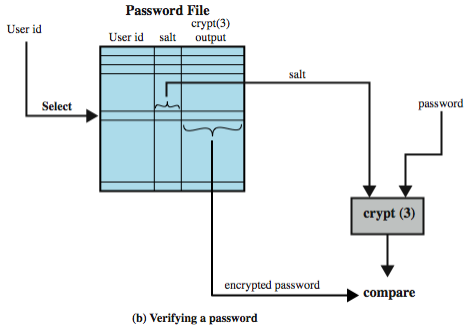


(a) Loading a new password

ثم يتم تخزين كلمة المرور المجزأة ، جنبًا إلى جنب مع نسخة نص عادي من القيمة المضافة ، في ملف كلمة المرور مقابل معرف المستخدم. لقد ثبت أن طريقة كلمة المرور المجزأة آمنة ضد مجموعة متنوعة من هجمات تحليل التشفير.

استخدام كلمات المرور المجزأة (Hashed passwords)

- عندما يحاول المستخدم تسجيل الدخول إلى نظام ما ، يقدم المستخدم معرفًا وكلمة مرور (كما هو موضح في الشكل (ب)). يستخدم نظام التشغيل المعرف للفهرسة في ملف كلمات المرور واسترداد نص القيمة المضافة وكلمة المرور المشفرة. يتم استخدام كلمة المرور التي يدخلها المستخدم والقيمة المضافة كمدخلات في روتين التشفير. إذا تطابقات النتيجة مع القيمة المخزنة ، يتم قبول كلمة المرور. هناك نوعان من التهديدات لنظام كلمة المرور هذا:
  - أولاً ، يمكن للمستخدم التمكن من جهاز باستخدام حساب ضيف
  - أو من خلال بعض الوسائل الأخرى ثم تشغيل برنامج تخمين كلمة المرور يسمى برنامج تكسير كلمة المرور على هذا الجهاز



(b) Verifying a password

بالإضافة إلى ذلك ، إذا كان الخصم قادرًا على الحصول على نسخة من ملف كلمات المرور ، فيمكن تشغيل برنامج تكسير على جهاز آخر اثناء فراغه، ويتيح هذا للخصم تشغيل الملايين من كلمات المرور المحتملة في فترة زمنية معقولة.

لماذا القيمة المضافة (salt value)

- تمنع ظهور كلمات المرور مكررة في ملف كلمات المرور
- تزيد من صعوبة هجمات القاموس
- يكاد يكون من المستحيل معرفة ما إذا كان شخص ما يستخدم نفس كلمة المرور على أنظمة متعددة

تكسير كلمة المرور

- **هجمات القاموس**: تنمية قاموس كبير لجميع كلمات المرور الممكنة
  - تجريب كل كلمة ومتغيراتها المحتملة في القاموس الكبير مع التجزئة في ملف كلمات المرور
  - هذا يعني أنه يجب تجزئة كل كلمة مرور باستخدام كل قيمة مضافة متاحة ثم مقارنتها بقيم التجزئة المخزنة.
  - إذا لم يتم العثور على تطابق ، فسيقوم برنامج الاختراق بمحاولة إجراء تغييرات على جميع الكلمات الموجودة في قاموس كلمات المرور المحتملة.
  - تشمل هذه الاختلافات تهجئة الكلمات إلى الوراء ، أو الأرقام الإضافية أو الأحرف الخاصة ، أو تسلسل الأحرف ،
- **هجمات جدول قوس قزح**: يُنشئ المهاجم قاموسًا كبيرًا لكلمات المرور المحتملة ، لكل كلمة مرور:
  - يولد المهاجم قيم التجزئة المرتبطة بكل قيمة مضافة ممكنة.
  - والنتيجة هي جدول ضخم لقيم التجزئة يُعرف بجدول قوس قزح. على سبيل المثال يقوم جدول 1.4 جيجا بتكسير 99.9٪ من كلمات مرور "ويندوز" الأبجدية في 13.8 ثانية
  - يمكن مواجهتها باستخدام قيمة مضافة كبيرة بدرجة كافية وطول تجزئة كبير بدرجة كافية.

نحو كلمة المرور افضل

- **مشاكل كلمات المرور** : يختار العديد من المستخدمين كلمة مرور قصيرة جدًا أو يسهل تخمينها. من ناحية أخرى ، إذا تم تعيين كلمات مرور للمستخدمين تتكون من ثمانية أحرف تم اختيارها عشوائيًا ، فإن اختراق كلمة المرور أمر مستحيل فعليًا، ولكن سيكون من المستحيل تقريبًا على معظم المستخدمين تذكر كلمات المرور الخاصة بهم.
- **الهدف**: هو القضاء على كلمات المرور التي يمكن تخمينها مع السماح للمستخدم بتحديد كلمة مرور يسهل تذكرها
- **التقنيات:**
  - **تعليم المستخدم**: يمكن إخبار المستخدمين بأهمية استخدام كلمات مرور يصعب تخمينها كما يمكن تزويدهم بإرشادات لاختيار كلمات مرور قوية. الإشكالية تحدث عندما يكون لديك عدد كبير من المستخدمين أو معدل تنقل المستخدمين كبير لأن العديد من المستخدمين سيتجاهلون الإرشادات ببساطة
  - **كلمات المرور المنشأة من النظام**: لها تاريخ من ضعف القبول من قبل المستخدمين ، فإذا كانت عشوائية بطبيعتها فلن يتذكرها المستخدمون ، وإذا كانت منطوقة فقد يميل المستخدم إلى تدوينها.
  - **التحقق التفاعلي من كلمة المرور** (فحص دوري): حيث يقوم النظام بشكل دوري بتشغيل أداة تكسير كلمات المرور الخاصة به للعثور على كلمات مرور يمكن تخمينها. يقوم النظام بإلغاء أي كلمات مرور يتم تخمينها وإخطار المستخدم بذلك. إنجازها يمكن أن يكلف في الموارد.
  - **التحقق الاستباقي من كلمة المرور** (في وقت الانشاء): حيث يختار المستخدم كلمة المرور الخاصة التي يقوم النظام بعد ذلك بفحصها لمعرفة ما إذا كان مسموحًا بها ، وإذا لم يكن الأمر كذلك ، يرفضها. يجب أن يكون هناك توازن بين قبول المستخدم وقوة كلمة المرور. من المحتمل أن يكون هذا الحل هو الأفضل.

المصادقة القائمة على الأداة المميزة

تسمى الاشياء التي يمتلكها المستخدم لغرض التحقق من المستخدم "الأدوات المميزة"، وتشمل هذه:

- **بطاقة منقوشة** :- أحرف مرفوعة في المقدمة ، على سبيل المثال بطاقة الائتمان القديمة
- **شريط مغناطيسي** :- شريط مغناطيسي في الخلف ، أحرف في المقدمة ، على سبيل المثال بطاقة مصرفية
- **بطاقة ذاكرة** :- بها ذاكرة إلكترونية بداخلها ، على سبيل المثال بطاقة الهاتف مسبقة الدفع
- **البطاقة الذكية** :- بها ذاكرة إلكترونية ومعالج بالداخل ، على سبيل المثال بطاقة الهوية البيو مترية (القياسات الحيوية) .

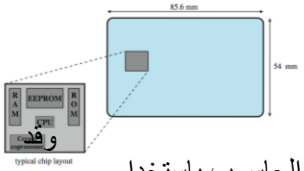
بطاقة الذاكرة

- يمكن لبطاقات الذاكرة تخزين البيانات ولكن لا يمكنها معالجتها. أكثر هذه البطاقات شيوعًا هي البطاقة المصرفية التي تحتوي على شريط مغناطيسي على ظهرها.
- يمكن للشريط المغناطيسي تخزين رمز أمان بسيط فقط ، والذي يمكن قراءته (ولسوء الحظ إعادة برمجته) بواسطة قارئ بطاقات غير مكلف. كما توجد بطاقات ذاكرة تحتوي على ذاكرة إلكترونية داخلية.
- بطاقة ذاكرة إلكترونية قد تستخدم وحدها للوصول المادي (على سبيل المثال: غرف الفنادق) وبعضها يحتوي على كلمة مرور/ رقم تعريف شخصي (على سبيل المثال: أجهزة الصراف الآلي)
- توفر بطاقة الذاكرة ، عند دمجها مع رقم التعريف الشخصي أو كلمة المرور أمانًا أكبر بكثير من كلمة المرور وحدها. يجب أن يكتسب الخصم الحيازة المادية للبطاقة (أو أن يكون قادرًا على نسخها) بالإضافة إلى معرفة رمز التعريف الشخصي.

بطاقة الذاكرة

- من بين العيوب المحتملة ما يلي:
  - **يتطلب قارئًا خاصًا**: يؤدي هذا إلى زيادة تكلفة استخدام الأداة المميزة ويخلق متطلبًا للحفاظ على أمان أجهزة وبرمجيات القارئ.
  - **فقدان الأداة**: تمنع الأداة المميزة المفقودة صاحبها مؤقتًا من الوصول إلى النظام. وبالتالي هناك تكلفة إدارية لاستبدال الأداة المفقودة. بالإضافة إلى ذلك ، إذا تم العثور على الأداة المميزة أو سرقتها أو تزويرها ، فلا يحتاج الخصم الآن إلا إلى تحديد رقم التعريف الشخصي للحصول على وصول غير مصرح به.
  - **استياء المستخدم**: على الرغم من أن المستخدمين قد لا يواجهون صعوبة في قبول استخدام بطاقة الذاكرة للوصول إلى أجهزة الصراف الآلي ، إلا أن استخدامها للوصول إلى الحاسوب قد يعتبر غير مريح.

البطاقة الذكية



- لها مظهر بطاقة الائتمان ، ولها واجهة إلكترونية ، تستخدم أيًا من بروتوكولات المصادقة الممكنة مع القارئ/الحاسوب باستخدام
  - كلمة مرور ثابتة : تشبه بطاقات الذاكرة.
  - ديناميكية : كلمات المرور التي يتم إنشاؤها كل دقيقة ؛ يتم إدخالها يدويًا عن طريق المستخدم أو إلكترونيًا
  - استجابة التحدي : ينشئ الحاسوب رقمًا عشوائيًا ؛ توفر البطاقة الذكية التجزئة الخاصة بها (على غرار – التشفير بالمفتاح العام).
- تحتوي البطاقة الذكية بداخلها على معالج دقيق كامل ، بما في ذلك المعالج والذاكرة ومنافذ الإدخال / الإخراج ، يتضمن بعضها دائرة معالجة مشتركة خاصة لعملية التشفير لتسريع مهمة تشفير الرسائل وفك تشفيرها أو إنشاء توقيعات رقمية للتحقق من صحة المعلومات المنقولة.
- في بعض البطاقات ، يمكن الوصول إلى منافذ الإدخال / الإخراج مباشرة بواسطة قارئ متوافق عن طريق تماسات اتصال كهربائية مباشرة. تعتمد البطاقات الأخرى بدلاً من ذلك على هوائي مضمن للاتصال اللاسلكي بالقارئ.

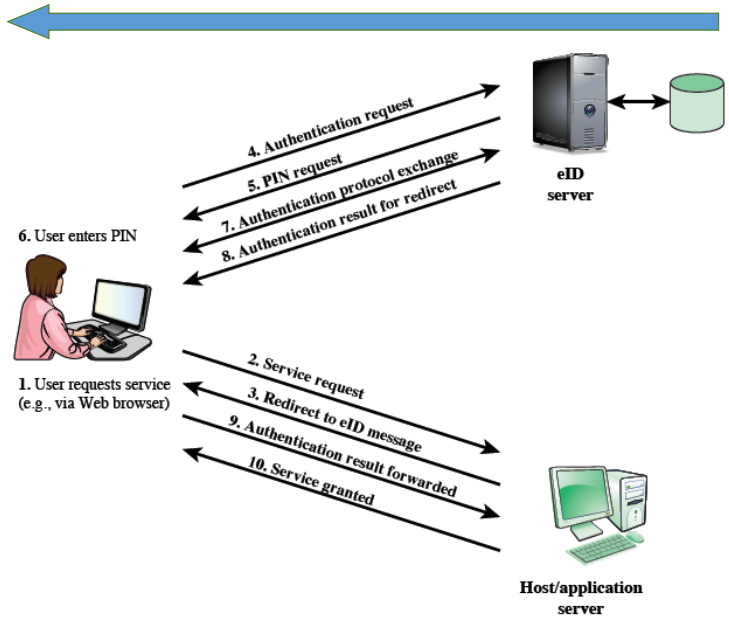
البطاقة الذكية

- تتضمن البطاقة الذكية النموذجية ثلاثة أنواع من الذاكرة.
  - تخزن ذاكرة القراءة فقط (ROM) البيانات التي لا تتغير خلال عمر البطاقة ، مثل رقم البطاقة واسم حامل البطاقة.
  - تحتوي ذاكرة القراءة فقط (EEPROM) القابلة للبرمجة وللمسح كهربائيًا على بيانات التطبيقات والبرامج ، مثل البروتوكولات التي يمكن للبطاقة تنفيذها وتحتوي أيضًا على بيانات قد تختلف بمرور الوقت.
  - تحتفظ ذاكرة الوصول العشوائي (RAM) بالبيانات المؤقتة التي يتم إنشاؤها عند تنفيذ التطبيقات.
- بديل البطاقة الذكية هو جهاز ذاكرة فلاش صغير وغير مكلف يُعرف باسم "دونجل فلاش" لها نفس وظيفة البطاقة الذكية ، ولكنها تتصل بمنفذ "USB" الموجود على الحاسوب ، وبالتالي فهي لا تحتاج إلى قارئ بطاقات معين.

بطاقة الهوية الالكترونية

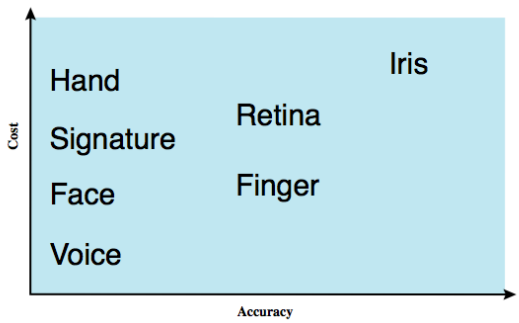
- تطبيق هام للبطاقات الذكية "الهوية الإلكترونية الوطنية" (eID) ، وتخدم نفس الغرض مثل بطاقات الهوية الوطنية الأخرى (على سبيل المثال ، رخصة القيادة) ، ويمكن أن تقدم إثباتًا أقوى للهوية
  - البطاقة ألالمانية (بيانات مطبوعة على البطاقة):
    - البيانات الشخصية (الاسم ، تاريخ الميلاد ، العنوان ، ...)، رقم الوثيقة (9- احرف ابجدية فريدة لكل بطاقة)، رقم الوصول إلى البطاقة (رقم عشوائي مكون من ستة أرقام: قد يستعمل ككلمة مرور) ، منطقة القراءة الآلية :نص من 3 اسطر(قد تستعمل ككلمة مرور)
    - الاستخدامات: (ePass) - الاستخدام الحكومي ، (eID) - الاستخدام العام ، (eSign) - يمكن أن يكون للمفتاح الخاص وشهادة مصادقة المفتاح .

التحقق من المستخدم بواسطة البطاقة الهوية الالكترونية (eID)



التحقق البيومتري (القياسات الحيوية)

- يحاول نظام المصادقة البيومترية التحقق من هوية الشخص بناءً على خصائصه الجسدية الفريدة ، والتي تشمل الخصائص الثابتة: مثل بصمات الأصابع وملامح راحة اليد وخصائص الوجه وأنماط شبكية العين وقزحية العين ؛ والخصائص الديناميكية: مثل البصمة الصوتية والتوقيع. بالمقارنة مع كلمات المرور والادوات المميزة ، تعتبر المصادقة البيومترية معقدة ومكلفة تقنيًا ، ولم تنضج بعد كأداة قياسية لمصادقة المستخدم على أنظمة الحاسوب. ويوضح الشكل التالي مؤشرًا تقريبيًا للتكلفة النسبية ودقة المقاييس الحيوية الأكثر شيوعًا:



- **خصائص الوجه**: تحديد الخصائص بناءً على الموقع النسبي وشكل ملامح الوجه الرئيسية ، مثل العينين والحاجبين والأنف والشفتين وشكل الذقن.

التحقق البيومتري (القياسات الحيوية)

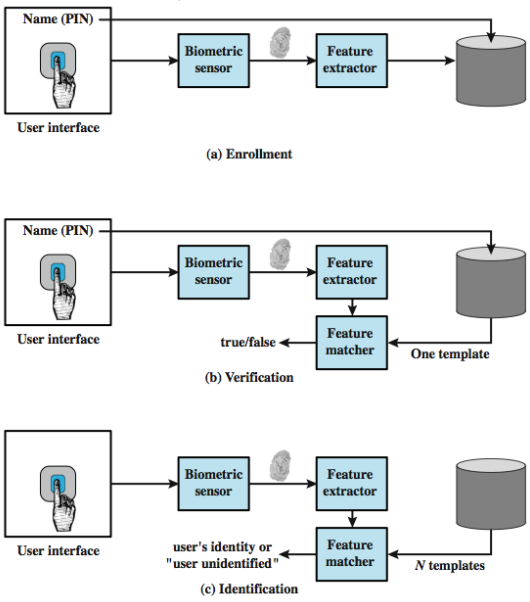
- **بصمات الأصابع**: نمط النتوءات والأخاديد الموجودة على سطح الإصبع ، ويعتقد أنها فريدة من نوعها بين جميع البشر. تستخرج أنظمة بصمات الأصابع الآلية عددًا من الميزات لاستخدامها كبديل للنمط الكامل.
- **تحديد ملامح اليد**: على سبيل المثال شكل وأطوال وعرض الأصابع.
- **نمط الشبكية**: يتكون من أوردة تحت سطح الشبكية فريد من نوعه وبالتالي فهو مناسب للتعرف عليه. يستخدم صورة رقمية لنمط الشبكية عن طريق عرض شعاع منخفض الكثافة من الضوء المرئي أو الأشعة تحت الحمراء في العين.
- **القزحية**: سمة فيزيائية فريدة أخرى هي البنية التفصيلية للقزحية.
- **التوقيع**: لكل فرد أسلوب فريد في الكتابة اليدوية ، ولا سيما في التوقيع.
- **الصوت**: ترتبط الأنماط ارتباطًا وثيقًا بالخصائص الفيزيائية والتشريحية للمتحدث ، ولكن لا يزال هناك اختلاف من عينة إلى أخرى بمرور الوقت من المتحدث نفسه ، مما يعقد مهمة التعرف على القياسات الحيوية.

كيفية عمل التحقق البيومتري (القياسات الحيوية)

يجب أولاً تسجيل كل شخص ليتم تضمينه في قاعدة بيانات المستخدمين المصرح لهم في النظام (مشابه لتخصيص كلمة مرور للمستخدم). بالنسبة لنظام المقاييس الحيوية ، يقدم المستخدم اسمًا ، وعادةً ما يكون نوعًا من كلمة المرور أو رقم تعريف شخصي للنظام. في نفس الوقت ، يستشعر النظام بعض الخصائص البيومترية لهذا المستخدم (مثل بصمة إصبع السبابة اليمنى). يقوم النظام برقمنة الإدخال ثم يستخرج مجموعة من الميزات التي يمكن تخزينها كرقم أو مجموعة من الأرقام التي تمثل هذه الخاصية الحيوية الفريدة ؛ ويشار إلى هذه المجموعة من الأرقام باسم "نموذج المستخدم". تم تسجيل المستخدم الآن في النظام ، والذي يحتفظ للمستخدم باسم معرف ، وربما رقم التعريف الشخصي أو كلمة المرور ، وقيمة المقاييس الحيوية. اعتمادًا على التطبيق ، تتضمن مصادقة المستخدم بنظام المقاييس الحيوية إما للتحقق أو لتحديد الهوية.

- يُعد **التحقق** مماثلاً لتسجيل دخول المستخدم إلى نظام ما باستخدام بطاقة ذاكرة أو بطاقة ذكية مقترنة بكلمة مرور أو رقم التعريف الشخصي . للتحقق من الهوية ، يقوم المستخدم بإدخال رقم التعريف الشخصي ويستخدم أيضًا مستشعر المقاييس الحيوية. يستخرج النظام الميزة المقابلة ويقارنها بالنموذج المخزن لهذا المستخدم. إذا كان هناك تطابق ، فإن النظام يصادق على هذا المستخدم.
- بالنسبة لنظام **تحديد الهوية** ، يستخدم الشخص مستشعر المقاييس الحيوية ولكنه لا يقدم معلومات إضافية. ثم يقارن النظام النموذج المقدم مع مجموعة النماذج المخزنة. إذا كان هناك تطابق ، فسيتم تحديد هوية هذا المستخدم. خلاف ذلك ، يتم رفض المستخدم.

كيفية عمل التحقق البيومتري (القياسات الحيوية)



يوضح الشكل كيفية تشغيل نظام القياسات الحيوية:

- **التحقق** مماثل لتسجيل دخول المستخدم عبر البطاقة الذكية ورقم التعريف الشخصي
- **تحديد الهوية** هي معلومات بيومترية ولكن بدون معرفات ؛ يقارن النظام مع القوالب المخزنة

المشاكل الأمنية لنظم مصادقة المستخدم

كما هو الحال مع أي خدمة أمن ، فإن التحقق من المستخدم ، ولا سيما التحقق من المستخدم البعيد ، يخضع لمجموعة متنوعة من الهجمات

- **هجمات العميل**: يحاول الخصم تحقيق مصادقة المستخدم دون الوصول إلى المضيف البعيد أو إلى التدخل في مسار الاتصالات
  - الخصم يحاول التنكر كمستخدم شرعي (على سبيل المثال في نظام قائم على كلمة المرور ، قد يحاول الخصم تخمين كلمة مرور المستخدم المحتملة).
  - الإجراء المضاد: كلمات مرور قوية ؛ الحد من عدد المحاولات.
- **هجمات المضيف**: يتم توجيه هجمات المضيف إلى ملف المستخدم في المضيف حيث يتم تخزين كلمات المرور أو رموز المرور المميزة أو نماذج المقاييس الحيوية
  - الإجراء المضاد: التجزئة وحماية قواعد بيانات كلمات المرور
- **التنصت**: يحاول المهاجم تعلم كلمات المرور من خلال مراقبة المستخدم ، والعثور على كلمات المرور المكتوبة ، وتسجيل نقرات المفاتيح وما إلى ذلك
  - التدابير المضادة الحرص على الاحتفاظ بكلمات المرور
  - مصادقة متعددة العوامل
  - مهمة المشرف: إبطال كلمات المرور المخترقة

المشاكل الأمنية لنظم مصادقة المستخدم

- **إعادة التشغيل**: تتضمن هجمات إعادة التشغيل خصمًا يكرر استجابة المستخدم التي تم التقاطها مسبقًا.
  - إجراء مضاد : بروتوكول الاستجابة والتحدي ، رموز المرور لمرة واحدة
- **حصان طروادة**: في هجوم حصان طروادة ، يتنكر تطبيق أو جهاز مادي كتطبيق أو جهاز أصلي بغرض التقاط كلمة مرور المستخدم أو رمز المرور أو المقاييس الحيوية. يمكن للخصم بعد ذلك استخدام المعلومات التي تم التقاطها للتنكر كمستخدم شرعي
  - الإجراء المضاد: مصادقة العميل ضمن بيئة أمنية موثوقة
- **منع الخدمة**: يحاول هجوم منع الخدمة تعطيل خدمة مصادقة المستخدم عن طريق إغراق الخدمة بمحاولات مصادقة عديدة.
  - الإجراء المضاد: مصادقة متعددة العوامل بأداة مميز